

# Configura VPN basata su route con route statica su FTD Gestito da FDM

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Procedura di configurazione in FDM](#)

[Verifica](#)

[Informazioni correlate](#)

---

## Introduzione

Questo documento descrive come configurare un sito basato su route statica per il tunnel VPN del sito su un FTD gestito da FDM.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza base del funzionamento di un tunnel VPN.
- Conoscenza preliminare della navigazione in Firepower Device Manager (FDM).

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Cisco Firepower Threat Defense (FTD) versione 7.0 gestito da Firepower Device Manager (FDM).

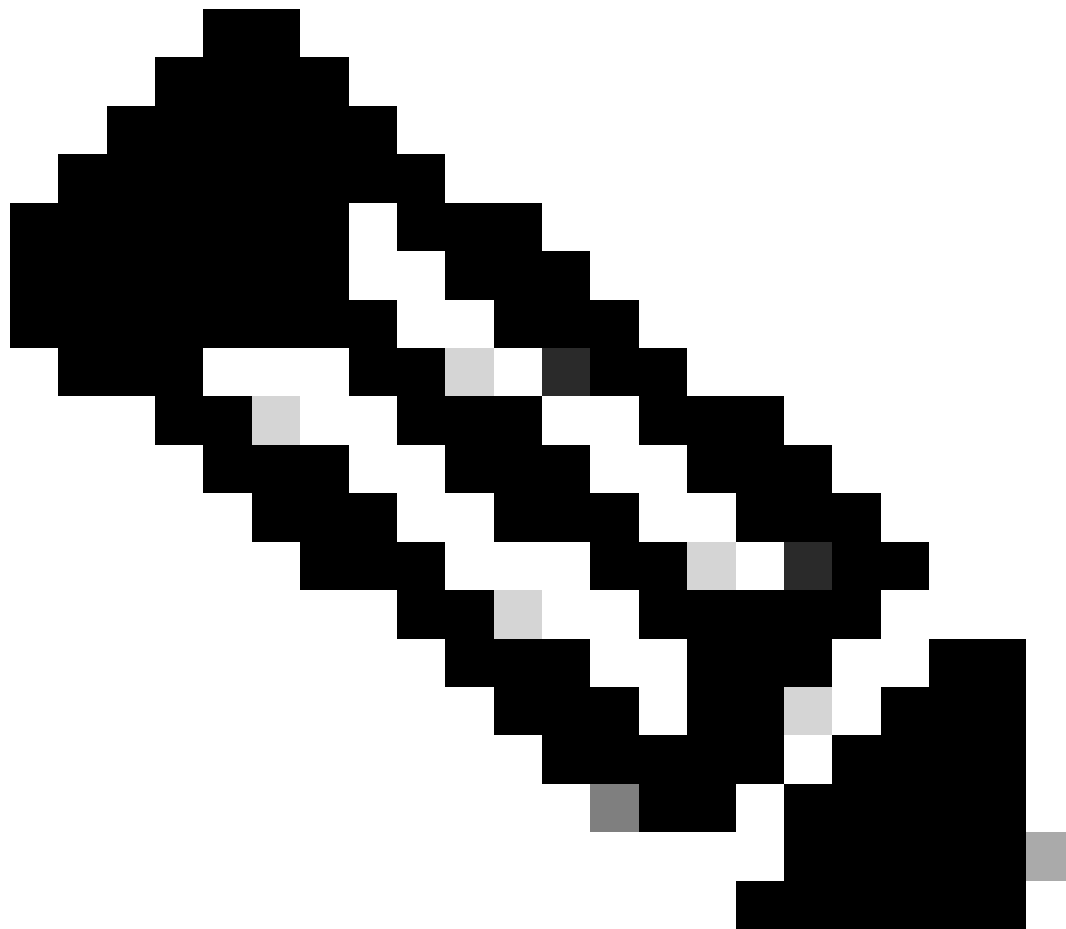
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Premesse

La VPN basata su route consente di determinare il traffico interessante da crittografare o inviare tramite il tunnel VPN e di utilizzare il routing del traffico anziché criteri/elenchi di accesso come nella VPN basata su criteri o su mappa crittografica. Il dominio di crittografia è impostato per consentire il traffico in entrata nel tunnel IPsec. I selettori di traffico locale e remoto di IPsec sono impostati su 0.0.0.0/0.0.0.0. Ciò significa che tutto il traffico instradato nel tunnel IPsec viene crittografato indipendentemente dalla subnet di origine/destinazione.

Nel documento si fa riferimento alla configurazione SVTI (Static Virtual Tunnel Interface).

---

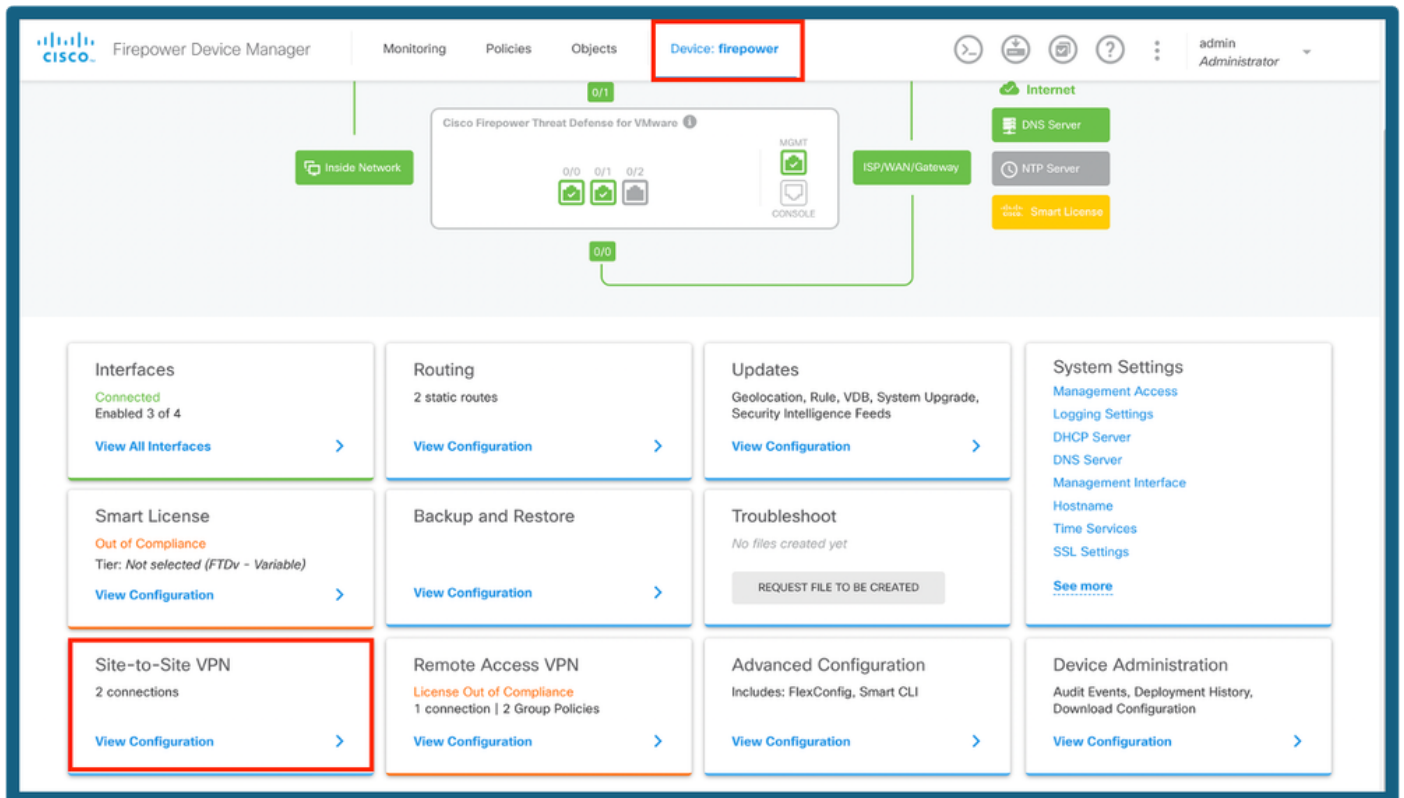


Nota: Non sono necessarie licenze aggiuntive. La VPN basata su route può essere configurata sia in modalità di licenza che in modalità di valutazione. Senza la conformità alla crittografia (funzionalità di esportazione controllate abilitate), solo DES può essere utilizzato come algoritmo di crittografia.

---

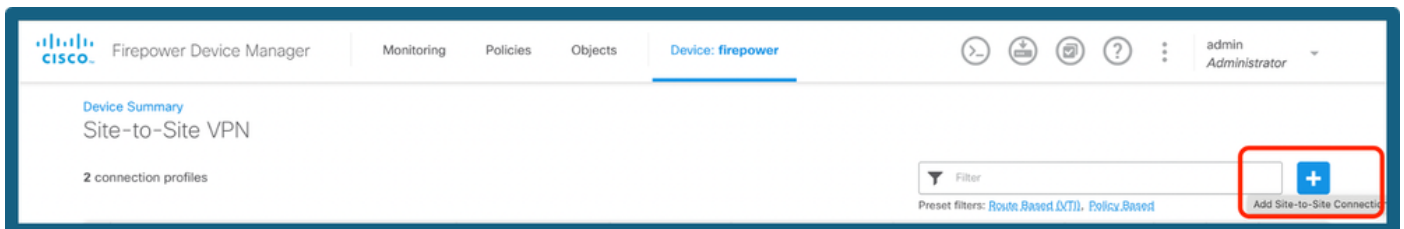
## Procedura di configurazione in FDM

Passaggio 1. Passare a Dispositivo > Da sito a sito.



Dashboard FDM

Passaggio 2. Fare clic sull'icona + per aggiungere un nuovo sito alla connessione.



Aggiungi connessione da sito a sito

Passaggio 3. Fornire un nome di topologia e selezionare il tipo di VPN come VTI (Route Based).

Fare clic su Local VPN Access Interface (Interfaccia di accesso VPN locale) e quindi su Create new Virtual Tunnel Interface (Crea nuova interfaccia tunnel virtuale) o selezionarne una dall'elenco esistente.

Firepower Device Manager | Monitoring | Policies | Objects | Device: firepower | admin Administrator

Local Network | FIREPOWER | VPN TUNNEL | INTERNET | OUTSIDE INTERFACE | PEER ENDPOINT | Remote Network

### Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: **vti-ipsec** | Type: **Route Based (VTI)** | Policy Based

Sites Configuration

**LOCAL SITE**

Local VPN Access Interface: Please select

Filter

Nothing found

[Create new Virtual Tunnel Interface](#)

**REMOTE SITE**

Remote IP Address

NEXT

Aggiungi interfaccia tunnel

Passaggio 4. Definire i parametri della nuova interfaccia del tunnel virtuale. Fare clic su OK.

Create Virtual Tunnel Interface

Name

tunnel10

Most features work with named interfaces only, although some require unnamed interfaces.

Status

☒

Description

Tunnel ID

10

0 - 10413

Tunnel Source

outside (GigabitEthernet0/0)

IP Address and Subnet Mask

192.168.1.1

/

255.255.255.252

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL

OK

Configurazione VTI

Passaggio 5. Scegliere la VTI appena creata o una VTI esistente in Virtual Tunnel Interface. Fornire l'indirizzo IP remoto.

New Site-to-site VPN

1 Endpoints 2 Configuration 3 Summary

Local Network FIREPOWER VPN TUNNEL INTERNET OUTSIDE INTERFACE PEER ENDPOINT Remote Network

### Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name:

Type: ☒ Route Based (VTI) ☐ Policy Based

Sites Configuration

LOCAL SITE

Local VPN Access Interface:

REMOTE SITE

Remote IP Address:

Aggiungi IP peer

Passaggio 6. Scegliere IKE Version, quindi il pulsante Edit (Modifica) per impostare i parametri IKE e IPsec come mostrato nell'immagine.

### IKE Policy

**i** IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

**IKE VERSION 2** ☒ **IKE VERSION 1** ☐

IKE Policy

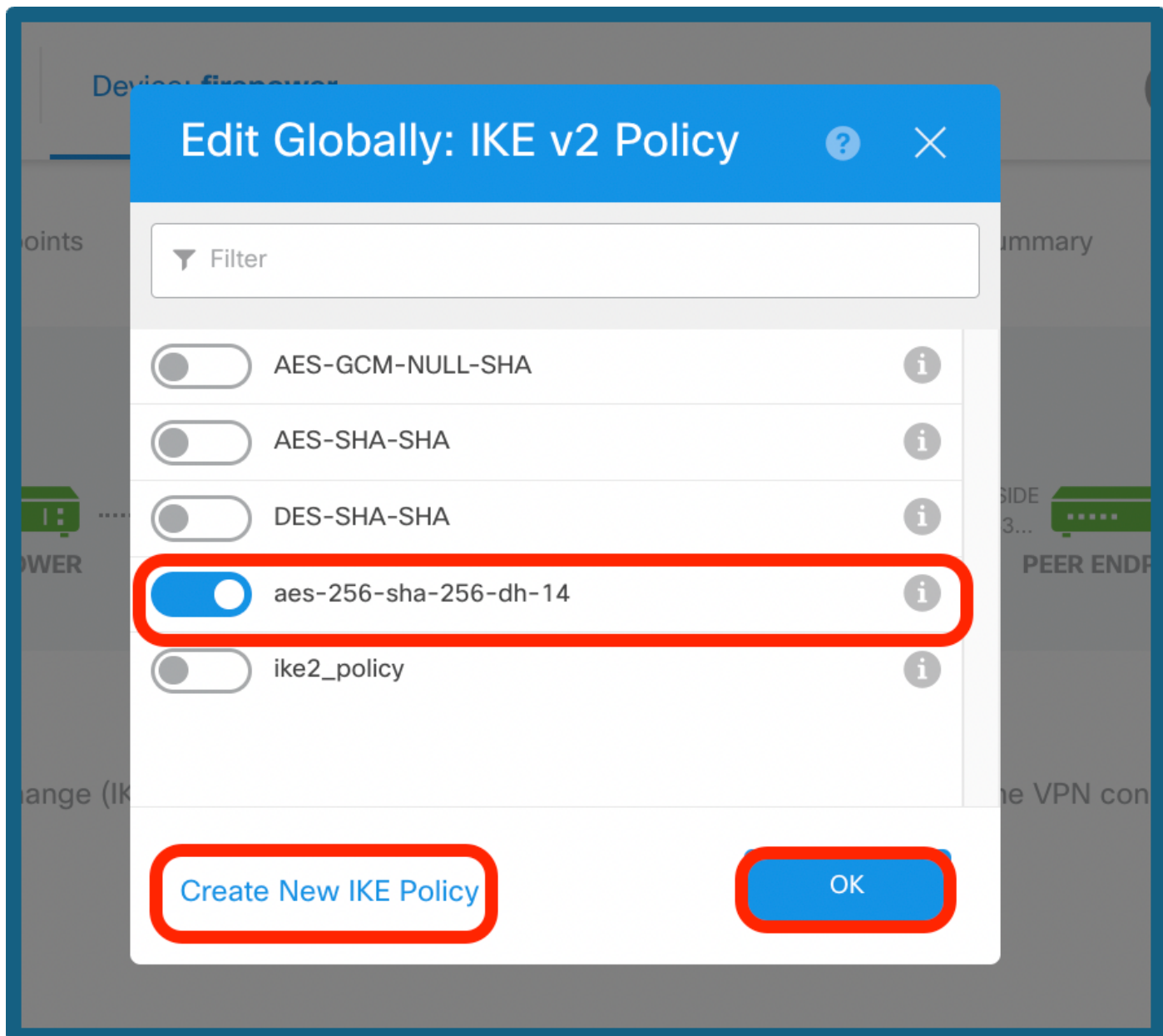
**Globally applied**

IPSec Proposal

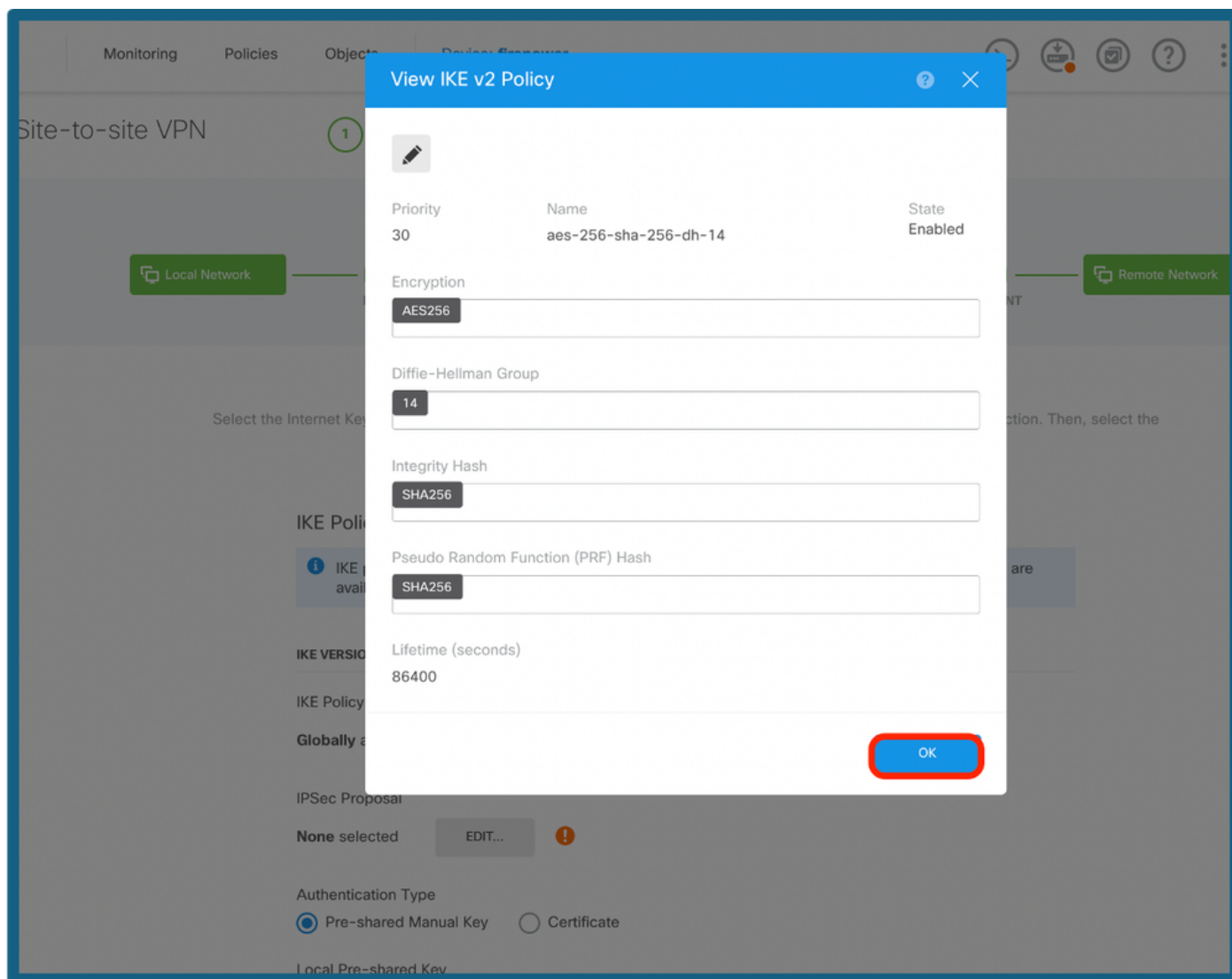
**Custom set selected**

Configura versione IKE

Passaggio 7a. Scegliere il pulsante Criterio IKE come illustrato nell'immagine e fare clic sul pulsante OK o su Crea nuovo criterio IKE per creare un nuovo criterio.

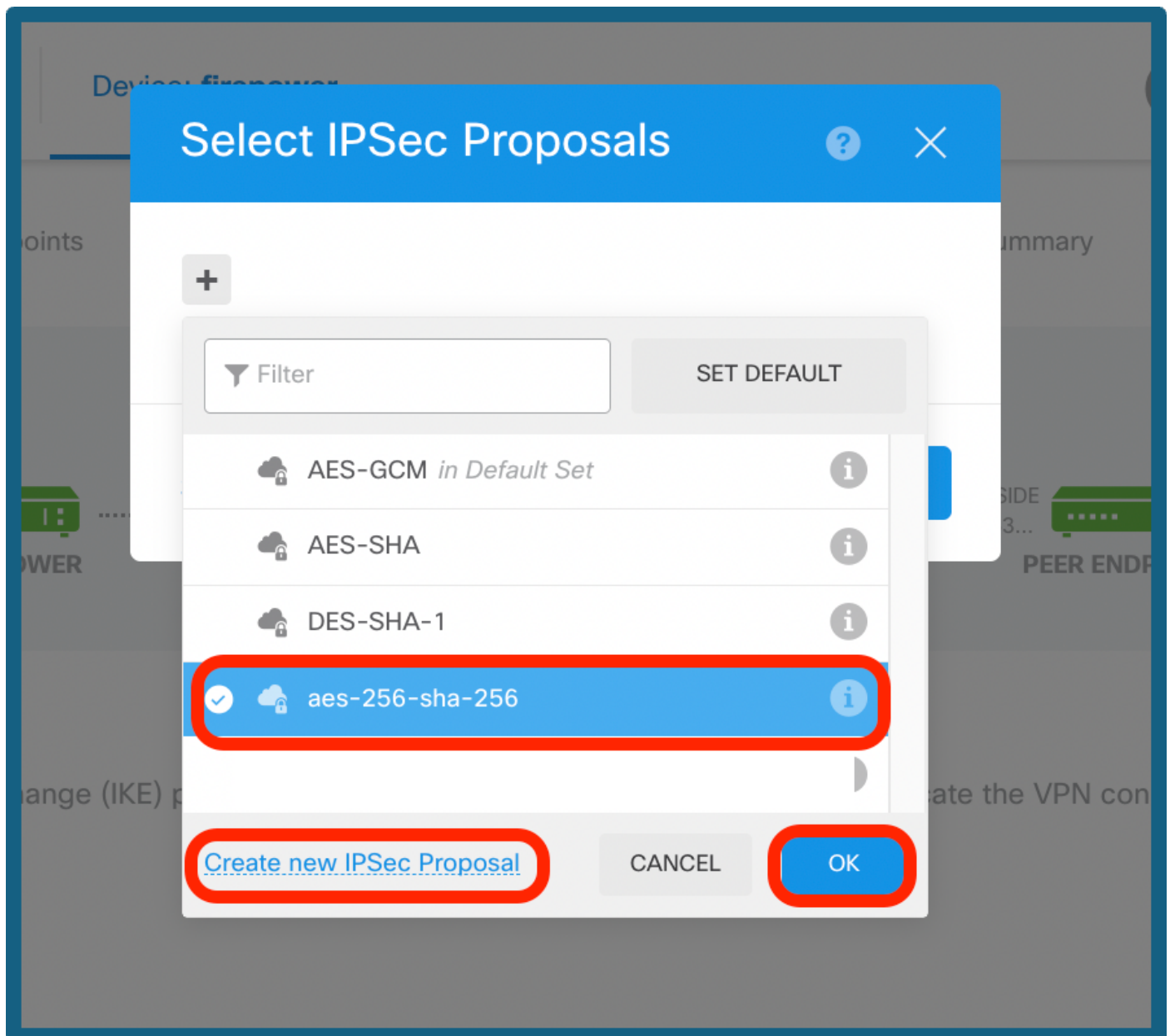


Scegli criterio IKE



Configurazione del criterio IKE

Passaggio 7b. Scegliere il pulsante Criterio IPsec come illustrato nell'immagine e fare clic sul pulsante OK o su Crea nuova proposta IPsec, se si desidera creare una nuova proposta.



Seleziona proposta IPsec

IKE v2 IPSec Proposal

Name  
aes-256-sha-256

Encryption  
AES256

Integrity Hash  
SHA256

OK

Configurazione della proposta IPSec

Passaggio 8a. Selezionare il tipo di autenticazione. Se si utilizza una chiave manuale già condivisa, specificare la chiave precondivisa locale e remota.

Passaggio 8b. (Facoltativo) Scegliere le impostazioni Perfect Forward Secrecy. Configurare i campi Durata IPSec e Dimensione durata, quindi fare clic su Avanti.

IKE VERSION 2 ☒

IKE VERSION 1 ☐

IKE Policy

Globally applied 

EDIT...

IPSec Proposal

Custom set selected 

EDIT...

Authentication Type

☒ Pre-shared Manual Key ☐ Certificate

Local Pre-shared Key

••••••••

Remote Peer Pre-shared Key

••••••••|

IPSEC SETTINGS

Lifetime Duration

28800

seconds

120 - 2147483647; (Default: 28800)

Lifetime Size

4608000

kilobytes

10 - 2147483647; (Default: 4608000).  
Leave empty for Unlimited.

Additional Options

Diffie-Hellman Group for Perfect Forward Secrecy

No Perfect Forward Secrecy (turned off)

BACK

NEXT

PSK e configurazione durata

Passaggio 9. Esaminare la configurazione e fare clic su Fine.

## Summary

Review your configuration. Click Finish to save the connection, or Back to edit settings. When you click Finish, this information will be copied to the clipboard so that you can save it and use it to configure the remote endpoint.

### Vti-Ipsec Connection Profile

 Peer endpoint needs to be configured according to specified below configuration.

**VPN Access  
Interface IP**  tunnel10 (1.1.1.1)



**Peer IP Address** 10.106.63.23

#### IKE V2

**IKE Policy** aes-256-sha256-sha256-14

**IPSec Proposal** aes-256-sha-256

**Authentication  
Type** Pre-shared Manual Key

#### IKE V1: DISABLED

#### IPSEC SETTINGS

**Lifetime  
Duration** 28800 seconds

**Lifetime Size** 4608000 kilobytes

#### ADDITIONAL OPTIONS

**Diffie-Hellman  
Group** Null (not selected)

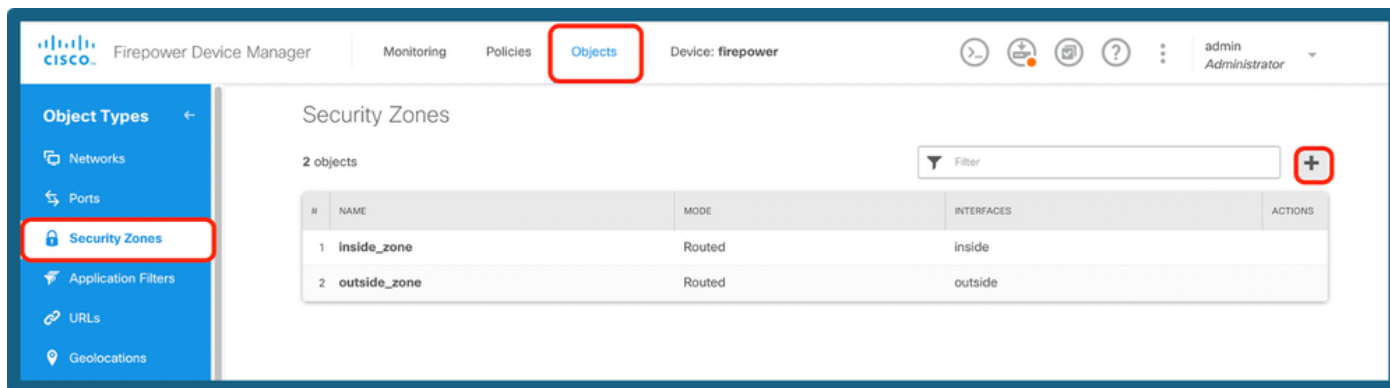
 Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

BACK

FINISH

Riepilogo configurazione

Passaggio 10a. Selezionare Oggetti > Aree di sicurezza, quindi fare clic sull'icona +.



Aggiungi area di sicurezza

Passaggio 10b. Create una zona e selezionate l'interfaccia VTI come mostrato di seguito.

### Add Security Zone

Name

vti-zone

Description

Mode

☒ Routed ☐ Passive

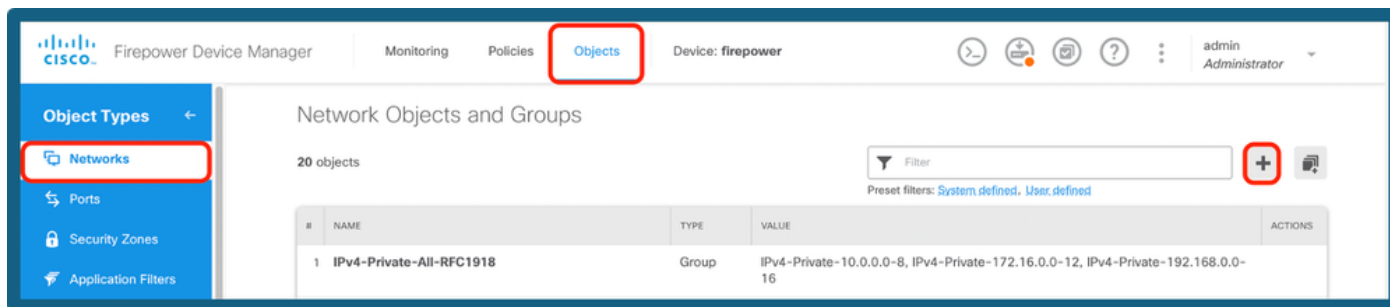
Interfaces

+ tunnel10 (Tunnel10)

CANCEL OK

Configurazione dell'area di protezione

Passaggio 11a. Selezionare Oggetti > Reti, quindi fare clic sull'icona +.



Aggiungi oggetti di rete

Passaggio 11b. Aggiungere un oggetto host e creare un gateway con l'ip del tunnel del peer-end.

### Edit Network Object

Name

vpn-gateway

Description

Type

☐ Network ☒ Host ☐ FQDN ☐ Range

Host

192.168.1.2

e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A

CANCEL OK

Configura gateway VPN

Passaggio 11c. Aggiungere la subnet remota e la subnet locale.

Edit Network Object

?

×

Name

remote-vpn-network

Description

Type

☒ Network

☐ Host

☐ FQDN

☐ Range

Network

172.16.10.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

Configurazione IP remoto

Edit Network Object

?

×

Name

inside-network

Description

Type

☒ Network

☐ Host

☐ FQDN

☐ Range

Network

10.10.10.0/24

*e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60*

CANCEL

OK

Configurazione IP locale

Passaggio 12. Passare a Periferica > Criteri e configurare i criteri di controllo di accesso.

**Add Access Rule**

Order: 1 | Title: vti-acl | Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

**SOURCE**

| Zones       | Networks       | Ports | SGT Groups |
|-------------|----------------|-------|------------|
| inside_zone | inside-network | ANY   | ANY        |
| vti-zone    | remote-vpn-... |       |            |

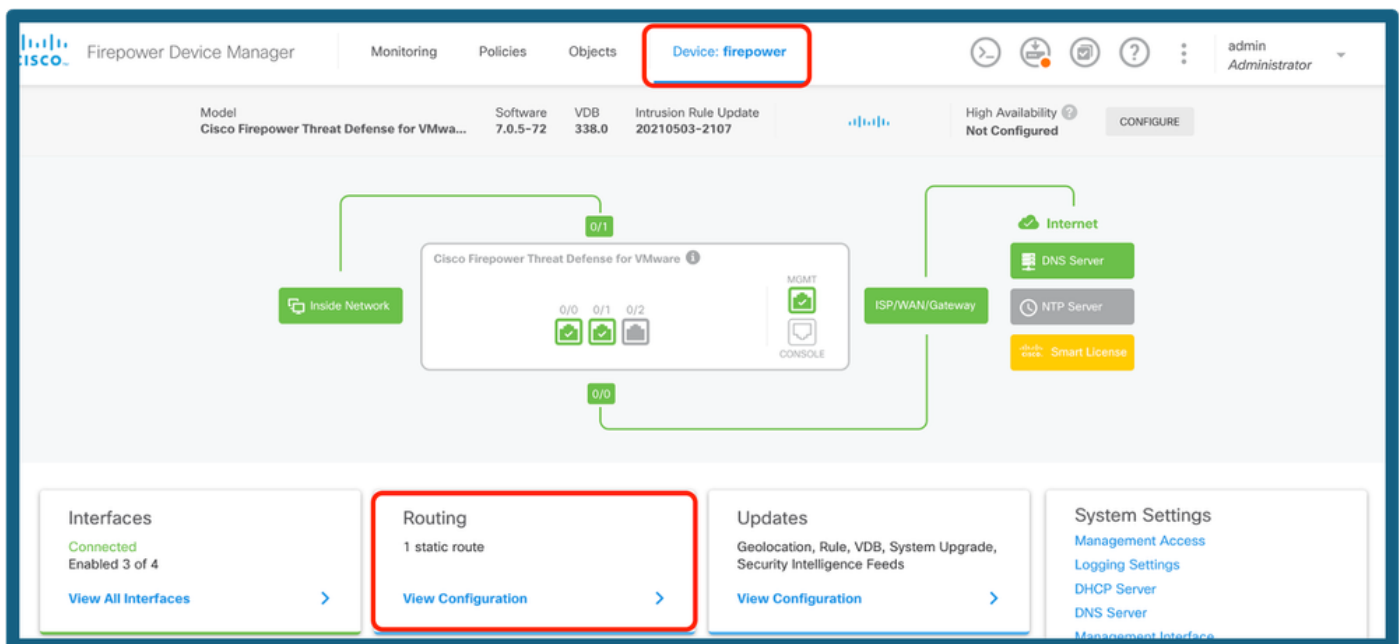
**DESTINATION**

| Zones       | Networks       | Ports | SGT Groups |
|-------------|----------------|-------|------------|
| inside_zone | inside-network | ANY   | ANY        |
| vti-zone    | remote-vpn-... |       |            |

Show Diagram: ☐ | CANCEL | OK

Aggiungi criteri di controllo di accesso

Passaggio 13a. Aggiungere il routing sul tunnel VTI. Selezionare Periferica > Instradamento.



Seleziona ciclo

Passaggio 13b. Passare a Instradamento statico nella scheda Instradamento. Fare clic sull'icona +.

Device Summary

## Routing

Add Multiple Virtual Routers

Static Routing BGP OSPF EIGRP ECMP Traffic Zones

1 route

Filter

| # | NAME    | INTERFACE | IP TYPE | NETWORKS  | GATEWAY IP  | SLA MONITOR | METRIC | ACTIONS |
|---|---------|-----------|---------|-----------|-------------|-------------|--------|---------|
| 1 | default | outside   | IPv4    | 0.0.0.0/0 | 10.106.52.1 |             | 1      |         |

Aggiungi route

Passaggio 13c. Fornire l'interfaccia, scegliere la rete, fornire il gateway. Fare clic su OK.

## Add Static Route

Name

vti-route

Description

Interface

tunnel10 (Tunnel10)

Protocol

☒ IPv4 ☐ IPv6

Networks

+

remote-vpn-network

Gateway

vpn-gateway

Metric

1

SLA Monitor

Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

Configura route statica

Passaggio 14. Passare a Distribuisci. Rivedere le modifiche, quindi fare clic su Deploy Now

(Distribuisci ora).

Pending Changes

Last Deployment Completed Successfully

26 Jun 2025 05:27 PM. [See Deployment History](#)

| Deployed Version (26 Jun 2025 05:27 PM)                               | Pending Version          |
|-----------------------------------------------------------------------|--------------------------|
| <div><div></div><div>Static Route Added: <i>vti-route</i></div></div> |                          |
| -                                                                     | metricValue: 1           |
| -                                                                     | ipType: IPv4             |
| -                                                                     | name: vti-route          |
| iface:                                                                |                          |
| -                                                                     | tunnel10                 |
| gateway:                                                              |                          |
| -                                                                     | vpn-gateway              |
| networks:                                                             |                          |
| -                                                                     | remote-vpn-network       |
| <div><div></div><div>Access Rule Added: <i>vti-acl</i></div></div>    |                          |
| -                                                                     | logFiles: false          |
| -                                                                     | eventLogAction: LOG_NONE |
| -                                                                     | ruleId: 268435458        |
| -                                                                     | name: vti-acl            |
| sourceZones:                                                          |                          |
| -                                                                     | vti-zone                 |
| -                                                                     | inside_zone              |
| destinationZones:                                                     |                          |
| -                                                                     | vti-zone                 |
| -                                                                     | inside_zone              |
| sourceNetworks:                                                       |                          |
| -                                                                     | remote-vpn-network       |
| -                                                                     | inside-network           |
| destinationNetworks:                                                  |                          |

MORE ACTIONS

CANCEL

DEPLOY NOW

Distribuire la configurazione

## Verifica

Una volta completata la distribuzione, è possibile verificare lo stato del tunnel sulla CLI utilizzando i seguenti comandi:

- 1. show crypto ikev2 sa
- 2. show crypto ipsec sa <ip-peer>

```
> show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

| Tunnel-id                                                                              | Local                                             | Remote           | Status | Role      |
|----------------------------------------------------------------------------------------|---------------------------------------------------|------------------|--------|-----------|
| 3294213359                                                                             | 10.106.52.222/500                                 | 10.106.63.23/500 | READY  | INITIATOR |
| Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK |                                                   |                  |        |           |
| Life/Active Time: 86400/141 sec                                                        |                                                   |                  |        |           |
| Child sa:                                                                              | local selector 0.0.0.0/0 - 255.255.255.255/65535  |                  |        |           |
|                                                                                        | remote selector 0.0.0.0/0 - 255.255.255.255/65535 |                  |        |           |
|                                                                                        | ESP spi in/out: 0x26a14554/0xd5db88bc             |                  |        |           |

```
> show crypto ipsec sa
```

```
interface: tunnel10
```

```
Crypto map tag: __vti-crypto-map-5-0-10, seq num: 65280, local addr: 10.106.52.222
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
current_peer: 10.106.63.23
```

Comandi show

## Informazioni correlate

Per ulteriori informazioni sulle VPN da sito a sito sull'FTD gestito da FDM, è possibile trovare la guida alla configurazione completa qui:

[Guida alla configurazione di FTD gestito da FDM](#)

### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).